REMARKS:

This paper is herewith filed in response to the Examiner's Office Action mailed on March 3, 2008 for the above-captioned U.S. Patent Application. This office action is a rejection of claims 1-6 of the application.

More specifically, the Examiner has rejected claim 1 under 35 USC 102(b) as anticipated by Walter (US6,151,677); rejected claims 1 and 4-5 under 35 USC 102(e) as being anticipated by Relander (US20020066012); and rejected claims 2-3 and 6 under 35 USC 103(a) as being unpatentable over Relander in view of Papineau (US7,092,703). The Applicant respectfully disagrees with the rejection.

Claims 1 and 5 have been amended for clarification. Claims 2-4 and6 have been amended to address formalities. Claims 7-11 have been added. Support for the new claims can be found at least on page 12, line 13 to page 14, line 12. No new matter is added.

Claim 1 recites:

> A system configured to arrange end-to-end (e2e) encryption between two or more pieces of terminal equipment communicating with one another, said terminal equipment comprising: a codec configured to convert an audio signal into a dataflow and vice versa, a module configured to manage encryption parameters stored in connection with the terminal equipment, an encryption key stream generator KSG configured to generate a key stream segment (KSS) with the said encryption parameters, a module configured to encrypt a dataflow and decrypt the encryption with the generated key stream segment, a module configured to synchronize the encrypted dataflow and to de-synchronize the synchronization, and at least one interface configured to receive the encryption parameters from the data communication network, and wherein at least one of the pieces of terminal equipment is configured to function as a special server terminal device, to manage and distribute at least the encryption parameters concerning a data communication network to the other pieces of terminal equipment based on an established criterion, and wherein the special server terminal device is configured to manage at least one of encryption and synchronization applications and to distribute these based on an established criterion to the other pieces of terminal

> equipment and the terminal equipment is configured to download and manage said applications, where the terminal equipment comprises a data memory configured to store the applications and a processor and operating memory configured to execute the applications.

Firstly, the Applicant submits that Walter does not relate to a terminal equipment downloading encryption and synchronization applications distributed by a special server terminal device as in claim 1.

As cited by the Examiner Walter discloses:

> "In accordance with further aspects of the present invention, the third processor comprises a memory, preferably a static RAM, for storing key exchange software received from the second processor responsive to the valid identification code, and the encryption engine comprises a memory, preferably a static RAM, containing traffic **encryption software received from the second processor** responsive to the valid identification code," (emphasis added), (col. 3, lines 38-45).

The Applicants notes that as cited Walter merely discloses an encryption engine wherein encryption software received from a second processor is stored in RAM. The Applicant notes that this cite from the Summary section in Walter is described in regards to Fig. 1 where Walter discloses:

> "The DSP 120 manages the user data interface in the data modes. A preferred DSP is the TMS320C50 manufactured by Texas Instruments. **Preferably, the DSP 120 has a memory 121, such as a static RAM, which stores key exchange software provided by the IC 130**," (emphasis added), (col. 5, lines 62-62).

The Applicant submits that as illustrated in Fig. 1 of Walter it can be seen that both the memory 121 and the IC 130 are embodied on a module 100 illustrated in Fig. 1. Thus, for at least this reason Walter can not be seen to disclose or suggest at least where claim 1 recites in part "the terminal equipment configured to **download and manage said applications**, where the terminal

equipment comprises a data memory configured to store the applications and a processor and operating memory configured to execute the applications."

The Applicant notes that Walter presents a method in which a security module has been arranged statically in connection with the terminal device. The security module includes a processor device in connection of which executed encryption program including encryption and decryption algorithms are also essentially static or at least in extremely inconveniently way updateable. The Applicant submits that apparently this is because the encryption program is a hardware level program, i.e. firmware (col. 3, line 50-51). Walter discloses that the encryption engine has been implemented in hardware (col. 3, lines 56-57) which also refers to the static nature of the encryption algorithms. Similarly, it is disclose that the security module has been arranged to a single integration circuit (col. 4, lines 65-67) which also refers to the static arrangement. Walter discloses that the security program (including encryption algorithms) is stored in smartcard IC. However, the smartcard IC has been integrated in this case statically to the security module on the device in Walter. The Applicant submits considering all of Walter it appears this implementation is performed to address security issues.

Walter discloses an essentially static environment to which the background section of the present application refers. An embodiment of the present invention is to arrange a dynamic security application and its operating environment to the terminal device. The present application discloses a system where the user can download to his or her terminal a desired security application. Further, a sufficient service, interface, and application environment has been arranged for the terminal to download security applications and to control them. The Applicant submits that this kind of application environment cannot be found in Walter. Furthermore, Walter does not mention how the updating of the security application of the terminal device would be dealt with.

The problems addressed by the present invention relate at least in part to difficulties faced by manufacturers in implementing encryption algorithms and methods used by the end users. The method of Walter cannot address this problem. In Walter, the terminal manufacturer must still

install in the terminal device the security applications used by the client/end user. Due to the static nature of Walter's solution, it appears that this has to be performed in the manufacturing phase of the terminal equipment. If these applications were not installed to a terminal device by the manufacturer, arranging of applications as a firmware implementation by a user would be considerably difficult, if even possible.

The Applicant contends that for at least these reasons Walter can not be seen to disclose or suggest at least where claim 1 recites in part "the terminal equipment is configured to **download and manage said applications**, where the terminal equipment comprises a data memory configured to store the applications and a processor and operating memory configured to execute the applications."

The Applicant submits that for at least the reasons stated Walter can not be seen to disclose or suggest claim 1 and the rejection of claim 1 should be removed.

Regarding the rejection of claim 1 over Relander the Applicant disagrees with the Examiner.

Firstly, the Applicant contends that Relander does not disclose or suggest at least where claim 1 relates to a "special server terminal device configured to manage at least one of **encryption and synchronization applications and to distribute these based on an established criterion** to the other pieces of terminal equipment."

As cited by the Examiner Relander discloses:

> "The key stream generator generates a key stream segment on the basis of a specific key and an initialisation vector. The keys are distributed to each terminal participating in the encrypted call. This forms part of the terminal equipment settings," (par. [0006]); and
>
> "The synchronization control is responsible for ensuring that both ends know the initialisation vector used with which each frame is encrypted. To allow the

> encrypter and the decrypter to agree on the value of the initialisation vector, a synchronisation vector is sent at the beginning of a speech item. [...] In addition to the initialisation vector, the synchronization vector comprises for example a key identifier and CRC error check to enable the terminal equipment to verify the integrity of the synchronization vector. The recipient thus counts the number of frames transmitted after the synchronization vector and on the basis of the last received initialisation vector and the number of the frames, the key stream generator generates a new initialisation vector," (par. [0007]).

The Applicant notes that here, as cited by the Examiner, what is disclosed is a key stream generator and a synchronization control. As stated above Relander discloses that the synchronization vector comprises a key identifier and a CRC error check. The Applicant submits that neither the keys nor the synchronization vector sent to a terminal in Relander can be seen to relate to an encryption or synchronization **application** as in claim 1. The Applicant contends that Relander does not disclose or suggest "special server terminal device configured to manage at least one of **encryption and synchronization applications and to distribute these based on an established criterion** to the other pieces of terminal equipment," as in claim 1.

Further, the Applicant submits that Relander can not be seen to disclose or suggest at least where claim 1 relates to **a terminal equipment configured to download and manage said applications** as in claim 1

Relander describes on [0004] that sender first encodes a voice sample to produce a plaintext sample. Using a specific key stream segment, the transmitting terminal creates an encrypted sample, which is transmitted to a network. With the same key stream segment the recipient then decrypts the encrypted sample to reproduce the plaintext sample. Key stream generator [0006] (located in the mobile station [0026]) generates a key stream segment on the basis of a specific key and an initialisation vector. The keys are distributed to each terminal participating in a call by the mobile station. Synchronization control [0007] (also located in a mobile station [0033]) is responsible for ensuring that both ends know the initialization vector. Synchronization vector including the initialisation vector is transmitted to each terminal participating the call by the mobile station at the beginning of speech item. The rest of Relander appears targeted to a

problem that occurs when an extra frame is added to a frame flow (for shifting a delay occurring in transfer of packets), and this problem is addressed in Relander.

The Applicant contends that for at least these reasons Relander can not be seen to disclose or suggest at least where claim 1 recites "the special server terminal device is configured **to manage at least one of encryption and synchronization applications** and **to distribute these based on an established criterion to the other pieces of terminal equipment** and **the terminal equipment configured to download and manage said applications.**"

Regarding the rejection of claim 5 the Applicant submits that for at least the reasons stated above Relander can not be seen to disclose or suggest at least where the apparatus of claim 5 relates to "a module configured to **download and manage at least one of dynamic encryption and synchronization applications.**"

Further, for at least the reasons already stated the Applicant submits that the references cited are not seen to disclose or suggest at least where claim 7 recites "receiving from a data communication network information comprising **at least one dynamic encryption application and at least one encryption key.**"

In addition, for at least the reasons stated the references cited are not seen to disclose or suggest at least where claim 11 recites "managing at least **dynamic encryption and synchronization applications**, and **distributing the applications based on an established criterion.**"

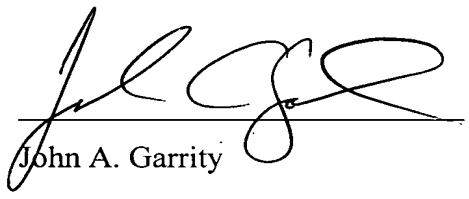
Papineau relates to a method to input and output data to/from Java MIDlets (abstract). Further, Papineau discloses that as a current security measure MIDlets downloaded and installed on a local file system can only access limited resources (col. 13, lines 4-18). Although the Applicant does not agree that a combination of Relander and Papineau is proper, the Applicant submits that such a combination would still address the deficiencies of Relander as stated above.

In addition, for at least the reason that claims 2-4, 6, and 8-10 depend from claims 1, 5, and 7 the references cited are not seen to disclose or suggest these claims.

Based on the above explanations and arguments, it is clear that the references cited cannot be seen to disclose or suggest claims 1-11. The Examiner is respectfully requested to reconsider and remove the rejections of claims 1-11 and to allow all of the pending claims 1-11 as now presented for examination.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record. Should any unresolved issue remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted:



6/30/08

John A. Garrity
Reg. No.: 60,470
Customer No.: 29683
HARRINGTON & SMITH, PC
4 Research Drive
Shelton, CT 06484-6212
Telephone: (203)925-9400
Facsimile: (203)944-0245
email: jgarrity@hspatent.com

Date

S.N.: 10/511,934
Art Unit: 2132

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

6-30-08 — Ann Okrentowicz

Date — Name of Person Making Deposit